

UNCLASSIFIED



# **NORTH DAKOTA HOMELAND SECURITY ANTI-TERRORISM SUMMARY**



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

UNCLASSIFIED

## **NDSLIC DISCLAIMER**

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

## **QUICK LINKS**

[NORTH DAKOTA](#)

[REGIONAL](#)

[NATIONAL](#)

[INTERNATIONAL](#)

[BANKING AND FINANCE  
INDUSTRY](#)

[CHEMICAL AND HAZARDOUS  
MATERIALS SECTOR](#)

[COMMERCIAL FACILITIES](#)

[COMMUNICATIONS SECTOR](#)

[CRITICAL MANUFACTURING](#)

[DEFENSE INDUSTRIAL BASE  
SECTOR](#)

[EMERGENCY SERVICES](#)

[ENERGY](#)

[FOOD AND AGRICULTURE](#)

[GOVERNMENT SECTOR  
\(INCLUDING SCHOOLS AND  
UNIVERSITIES\)](#)

[INFORMATION TECHNOLOGY  
AND TELECOMMUNICATIONS](#)

[NATIONAL MONUMENTS AND  
ICONS](#)

[POSTAL AND SHIPPING](#)

[PUBLIC HEALTH](#)

[TRANSPORTATION](#)

[WATER AND DAMS](#)

[NORTH DAKOTA HOMELAND  
SECURITY CONTACTS](#)

UNCLASSIFIED

## **NORTH DAKOTA**

**Fargo police investigate copper theft.** Fargo, North Dakota police investigated a huge copper theft the weekend of December 17 and 18 that may be connected to several other recent break-ins. A police lieutenant said thieves stole 52 large spools of copper from Dakota Electric Construction. The missing metal is valued at \$100,000. This was the second major copper theft in the Fargo area. Investigators are trying to figure out if the recent Fargo copper thefts are connected to others around the area, including one in Wahpeton, and \$30,000 in copper missing from a Jamestown business. Source:

[http://www.kfyrtv.com/News\\_Stories.asp?news=54013](http://www.kfyrtv.com/News_Stories.asp?news=54013)

## **REGIONAL**

**(Minnesota) Three shot at courthouse in northern Minnesota.** A man found guilty of a sex crime shot a county prosecutor at the Cook County Courthouse in Grand Marais, Minnesota, three times, and a second man multiple times before he was caught, authorities said December 16. A 42-year-old man was arrested shortly after the December 15 shooting, and was being held in the county jail, the state public safety department said. The Cook County attorney shot twice in the abdomen and once in the groin was in fair condition, and was recovering after surgery, said a hospital spokeswoman. A second man was listed in good condition at a hospital December 16 after also sustaining multiple gunshot wounds. A third person was treated and released from an area hospital December 15. The suspect was found guilty December 15 of a sex crime in a jury trial. The judge was talking with jurors in the courtroom at the small courthouse after the conclusion of the trial when they heard shots fired in another part of the courthouse. The Cook County Courthouse does not have metal detectors. It remained closed December 16 as the investigation continued. Source: [http://news.yahoo.com/three-people-shot-courthouse-northern-minnesota-010306185.html;\\_ylt=AkSW7cKMtRpWnmeF9FbuGclvzwcF;\\_ylu=X3oDMTNuY2ZoazlmBG1pdANUb3BTdG9yeSBVU1NGBHBrZwMzN2UxZmNiZS04ZGM0LTm2NTQtYTcxMy1iNzMzNDQ0NzdjYzlEcG9zAzEEc2VjA3RvcF9zdG9yeQR2ZXIDN2Q](http://news.yahoo.com/three-people-shot-courthouse-northern-minnesota-010306185.html;_ylt=AkSW7cKMtRpWnmeF9FbuGclvzwcF;_ylu=X3oDMTNuY2ZoazlmBG1pdANUb3BTdG9yeSBVU1NGBHBrZwMzN2UxZmNiZS04ZGM0LTm2NTQtYTcxMy1iNzMzNDQ0NzdjYzlEcG9zAzEEc2VjA3RvcF9zdG9yeQR2ZXIDN2Q)

**(Nebraska) Copper thieves hit food bank building.** Food Bank for the Heartland officials in Omaha, Nebraska said December 19 they are dealing with almost \$100,000 worth of repairs after copper thieves broke into their old building. Just as the food bank was about to sell its old building, it got the news that thieves went hunting for copper there. According to police, the thieves went over a barbed-wire fence, climbed up onto the roof, and shredded the building's HVAC system. Source: <http://www.ketv.com/news/30034464/detail.html>

**(South Dakota) Releases reduced to a trickle at Gavins Point.** A source of flooding along the Missouri River in the summer of 2011 has nearly dried up, KTIV 4 Sioux City reported December 18. Releases were reduced to 20,000 cubic feet per second (CFS) at Gavins Point Dam in Yankton, South Dakota. That is down from the 160,000 CFS at the height of the flood. It was so low that only one of the 14 floodgates was open. The U.S. Army Corps of Engineers plans to

## UNCLASSIFIED

keep the current releases through the winter. Source:

<http://www.ktiv.com/story/16349704/gavins-point-dam-releases-hold-steady-for-winter>

### **NATIONAL**

**Panel: Corps not to blame for Missouri River flood.** The U.S. Army Corps of Engineers did what it could with the record flooding on the Missouri River in 2011, although proposed changes could help avoid a disastrous repeat, especially since such floods could become more frequent, an expert panel said in a report released December 20. The 99-page analysis said “climatic extremes” appear to be getting “bigger and more frequent,” with the experts calling for updated flood probability models and procedures. It did not cite climate change as a factor, saying the issue was “beyond the scope of this report.” The Corps said the floods caused \$630 million in damage to levees, dams, and channels built to control the river. The Corps manages the 2,341-mile-long river, which flows from Montana through North Dakota, South Dakota, Nebraska, Kansas, Iowa, and Missouri. The report said the 2011 flood was the “the largest of the period of record in terms of runoff volume, and it stressed the mainstream reservoir system and its operators as never before.” An expert from the panel said May rainfall in Montana exceeded 300 percent of normal, surprising everyone and causing the biggest problems. However, he said such unusual weather may be a more common part of the weather cycle. The experts said their first suggestion would be to ensure more federal money is available to repair and maintain the current system of spillways, tunnels, and other infrastructure. Other recommendations included improved monitoring of pending snowmelt in Plains states, as is done in the northern Rocky Mountain that feed the river. They also suggested better collaboration with weather forecasting and water monitoring agencies, improved monitoring systems for tributaries, and an update of the master manual that guides management for all authorized uses on the river. Source: <http://www.sacbee.com/2011/12/20/4135383/panel-corps-not-to-blame-for-missouri.html>

**Truck thieves take millions in electronics.** Police said December 17 they suspect four or five people were involved in the theft of almost \$2 million in electronics when a truck driver discovered his tractor trailer missing from a rest stop. A Chesterfield, Indiana police officer said the cab of the missing truck was found within a half mile of where it was taken, but its trailer containing more than 5,000 Blackberry Playbook tablets is still missing. The officer said he thought the theft of the 2007 Volvo truck December 15 on its way to Waterloo, Canada, was very well planned. The cab of the truck had been parked amid a crowd of semis not far from the Pilot Travel Plaza where the driver stopped to eat and take a shower. Police said the thieves evidently had a truck of their own waiting to take away the trailer. The driver had picked up the playbooks from the Brightpoint company in Plainfield, Indiana. Police have surveillance video of two men watching the driver during the stop, the officer said. Further investigation led police to believe two or three other individuals were involved. The officer said police hope to make an arrest in the case because they retrieved fingerprints. Source: [http://news.yahoo.com/truck-thieves-millions-electronics-173357173.html;\\_ylt=AozEjI3VwfaKY.UEFetvHglvzwcF;\\_ylu=X3oDMTNvcM5iMDZvBG1pdANUb3](http://news.yahoo.com/truck-thieves-millions-electronics-173357173.html;_ylt=AozEjI3VwfaKY.UEFetvHglvzwcF;_ylu=X3oDMTNvcM5iMDZvBG1pdANUb3)

## UNCLASSIFIED

[BTdG9yeSBVU1NGBHBrZwNiMGZhMjE2Yi03YWJmLTM0OTYtYThjOC1iZWJlODA5MDZiOWUEcG9zAzEyBHNIYwN0b3Bfc3RvcnkEdmVyAzlkY2M2OWYwLTl4](http://BTdG9yeSBVU1NGBHBrZwNiMGZhMjE2Yi03YWJmLTM0OTYtYThjOC1iZWJlODA5MDZiOWUEcG9zAzEyBHNIYwN0b3Bfc3RvcnkEdmVyAzlkY2M2OWYwLTl4)

## **INTERNATIONAL**

**IAEA has grave concerns.** The International Atomic Energy Agency (IAEA) conveyed to Japan its grave concern over not being informed about nuclear substances found in the waste of domestic facilities subject to the agency's inspections, government officials said. The IAEA expressed its concern to Japan in February, and has made a rare request to also examine waste that is usually not subject to its inspections, the Japan Times reported December 17. In October 2010, large quantities of unreported highly enriched uranium and plutonium were found in nuclear waste at a research and development center. Source:

[http://www.japantimes.co.jp/rss/nn20111217a5.html?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed:+japantimes\\_news+\(The+Japan+Times+Headline+News+-+News+&+Business\)](http://www.japantimes.co.jp/rss/nn20111217a5.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+japantimes_news+(The+Japan+Times+Headline+News+-+News+&+Business))

**Russia seizes Iran-bound radioactive material.** Russia's customs service said December 16 it had seized radioactive sodium-22, an isotope that is used in medical equipment but has no weapons use, from the luggage of a passenger planning to fly from Russia to Iran. The service said in a statement that the material could be obtained only "as a result of a nuclear reactor's operations" but did not say when it had been discovered at Moscow's Sheremetyevo international airport. The material triggered an alarm in the airport's radiation control system, and a luggage search led to the discovery of 18 pieces of the radioactive metal packed in individual steel casings, it said. The passenger boarded the plane for Tehran and left Russia, the customs service said. It added that the passenger was an Iranian national. Russian law enforcement agencies opened a criminal investigation into the incident. Sodium-22 can be used for calibrating nuclear detectors and in medical equipment, nuclear experts said. Source:

<http://www.reuters.com/article/2011/12/16/us-russia-iran-radioactive-idUSTRE7BF0PH20111216>

**Fukushima is in cold shutdown, says Japanese prime minister.** Japan's prime minister December 16 announced that the Fukushima nuclear power plant had been brought to a state of "cold shutdown", a significant step towards resolving the crisis, 9 months after it was struck by a powerful earthquake and tsunami. Cold shutdown is achieved when the temperature of water used to cool nuclear fuel rods remains below boiling point and radiation emitted by the reactors is no higher than the government-set limit for the public of one millisieverts a year. The plant's operator managed to bring water temperatures to below boiling point for the first time in September. Officials said the temperatures inside reactors number one to three, which all suffered meltdown, now range from 38C to 68C (100F to 154F.) Source:

<http://www.guardian.co.uk/world/2011/dec/16/fukushima-cold-shutdown-japanese-pm1?newsfeed=true>

## **BANKING AND FINANCE INDUSTRY**

**USAA warns members of sophisticated phishing scam.** USAA is warning its members about a sophisticated phishing scam that attempts to install a malicious banking Trojan on members computers. The Texas-based financial services association issued a notice to members December 19 about what it described as an “aggressive email phishing scam” directed at USAA members. The phishing e-mails have the subject line “Deposit Posted” and even include a randomly generated four digit “Security Zone” number that mimics the customer’s actual USAA member number, the firm said. USAA said the e-mail messages do not contain malicious links, but do ask members to open an attachment that, once opened, will install a “malicious banking virus” designed to steal user account information and that would “require a complete reinstall of your computers (sp) operating system.” Source: [http://threatpost.com/en\\_us/blogs/usaa-warns-members-sophisticated-phishing-scam-121911](http://threatpost.com/en_us/blogs/usaa-warns-members-sophisticated-phishing-scam-121911)

**Influential Ukrainian general arrested for international cybercrimes.** The FBI in collaboration with the Romanian Intelligence Service (SRI) apprehended a 54-year-old Ukrainian retired general and two of his accomplices while they were trying to withdraw \$1 million from CEC Bank, money obtained as a result of cyberfraud. The former general, an Israeli business man, and a 37-year-old Moldavian were arrested December 16 in Iasi, Romania, while they were trying to obtain the money, reports local newspaper Adevarul. After they managed to obtain Internet banking account credentials belonging to business owners from Italy and the United States, the group transferred large sums of money into the accounts of companies they owned. “Later, to wash the money trail, fictitious commercial transactions were made, while in reality the funds were being transferred to other accounts or withdrawn in cash by the members of the criminal group,” reads a statement from Romanian anti-crime and terrorism unit DIICOT. A day before the operation was busted, the three men tried to withdraw from the same financial institution the sum of \$450,000, which they obtained from the accounts of an Italian company. Since the men looked suspicious, the bank postponed the transaction and alerted authorities. The general, who has been living in Belgium for the past few years, claims the \$1 million was given to him by a company that wanted to buy shares at the TV station he owned. Source: <http://news.softpedia.com/news/Influential-Ukrainian-General-Arrested-for-International-Cybercrimes-241298.shtml>

**U.S. government blames Hezbollah for role in \$300 million money laundering scheme.** Federal authorities blamed Lebanese financial institutions December 15 for wiring more than \$300 million into the United States in a money-laundering scheme they said used the U.S. financial system to benefit the militant group Hezbollah. The U.S. government said in the lawsuit filed in a Manhattan, New York federal court it seeks nearly a half-billion dollars in money-laundering penalties from some Lebanese financial entities, 30 U.S. car buyers, and a U.S. shipping company. It also said it is entitled to claim their assets as forfeitable under U.S. money-laundering laws. Prosecutors said the \$300 million was wired from Lebanon to the United States, and was used to buy used cars and ship them to West Africa. They said Hezbollah money-laundering channels were used to ship proceeds from the car sales and narcotics trafficking back to Lebanon. The accusations came 2 days after an indictment in federal court in



## UNCLASSIFIED

Alexandria, Virginia, accused a fugitive of leading a drug conspiracy that provided income for Hezbollah, an Iranian-backed Lebanese militant group the U.S. has branded a terrorist organization. Source: [http://www.washingtonpost.com/national/us-government-blames-hezbollah-for-role-in-300-million-money-laundering-scheme/2011/12/15/gIQAL3MgwO\\_story.html](http://www.washingtonpost.com/national/us-government-blames-hezbollah-for-role-in-300-million-money-laundering-scheme/2011/12/15/gIQAL3MgwO_story.html)

**(Utah) U.S. Ponzi scheme targeted Mormons: SEC.** U.S. financial regulators charged a father and son in Utah December 16 with operating a \$220-million property investment Ponzi scheme that targeted fellow members of the Mormon church. The Securities and Exchange Commission (SEC) charged the pair with selling shares in their purported real estate business, and using the funds from some investors to pay returns promised to others. The SEC said that since 2008, the two solicited investments into their business of ostensibly buying, rehabilitating, and then renting out properties. The pair appeared to use the memberships in the Utah-based Church of Jesus Christ of Latter-Day Saints — the Mormon church — "to make connections and win over the trust of prospective investors," the SEC said. Securities were sold without registering with the SEC as required by law. Moreover, the funds raised were often not used for investing into properties, with some moved from one entity to another to keep investors happy while the entities lost money. "They have essentially been operating a shell game intended to raise additional funds from new or existing investors in order to meet the rapidly growing financial obligations of their operation," the SEC said. Source: [http://www.google.com/hostednews/afp/article/ALeqM5j0OqG\\_xudf2MhfOrzOHlbnvYD7NvA?docId=CNG.903f8dc21dad4620c0e41129a8b95585.671](http://www.google.com/hostednews/afp/article/ALeqM5j0OqG_xudf2MhfOrzOHlbnvYD7NvA?docId=CNG.903f8dc21dad4620c0e41129a8b95585.671)

## **CHEMICAL AND HAZARDOUS MATERIALS SECTOR**

**Nuclear regulator slow in correcting information security vulnerabilities, says audit.** An audit found the Nuclear Regulatory Commission (NRC) cannot secure its own networks, Infosecurity reported December 16. The audit commissioned by the NRC Inspector General found the commission's plans of action and milestones for the remediation of information security vulnerabilities often did not contain all known security vulnerabilities and remained open past their due date. In addition, agency staff sometimes declared the vulnerabilities to be resolved without sufficient evidence. A security test found that many network components had never been security hardened, and that many patches had not been installed. The problems with patching indicated either that the agency's patching solution had not been properly configured or that personnel responsible for those system components had not requested downloads of the patches from the enterprise-wide patching system, the audit said. Source: <http://www.infosecurity-magazine.com/view/22743/nuclear-regulator-slow-in-correcting-information-security-vulnerabilities-says-audit/>

**NRC approves prioritization of Japan lessons-learned task force recommendations.** The Nuclear Regulatory Commission announced December 16 it approved the staff's prioritization of the Near-Term Task Force recommendations on lessons learned from the incident at the Fukushima Daiichi nuclear plant in Japan, and supports action on the Tier 1 and Tier 2 recommendations. Tier 1 recommendations are those Task Force recommendations the staff

## UNCLASSIFIED

## UNCLASSIFIED

determined could be implemented without unnecessary delay, and for which sufficient resources are available. Tier 2 includes recommendations that cannot be initiated in the near term due to factors that include the need for further technical assessment and alignment, dependence on Tier 1 issues, or availability of critical skill sets. Source:

[http://www.pennenergy.com/index/power/display/9839613443/articles/pennenergy/power/nuclear/2011/december/nrc-approves\\_prioritization.html](http://www.pennenergy.com/index/power/display/9839613443/articles/pennenergy/power/nuclear/2011/december/nrc-approves_prioritization.html)

### **COMMERCIAL FACILITIES**

**(New York) More than 50 'Occupy' protestors arrested in New York.** More than 50 anti-Wall Street protestors in New York City were arrested December 17 after they tried to climb over a chain-link fence around a church parking lot in a bid to establish a new encampment. The demonstrators used a wooden ladder to scale a chain-link fence into the lot owned by Trinity Church, an Occupy Wall Street spokesman said. Police had no immediate figure on how many people were taken into custody, but the president of the New York City chapter of the National Lawyers Guild, put the number at about 55. The remaining demonstrators marched through Manhattan's streets toward the house of the Trinity Church rector, but were turned away by police. A church official said the vacant church lot the OWS wanted to move into "has no facilities to sustain a winter encampment. In good conscience and faith, we strongly believe" erecting a camp there "would be wrong, unsafe, unhealthy, and potentially injurious." Source:

[http://news.yahoo.com/more-50-occupy-protesters-arrested-york-005726648.html;\\_ylt=AoKhxZ16PZLhp2CNMZgCIJlvzwcF;\\_ylu=X3oDMTNucXRyaDBvBG1pdANUb3BTdG9yeSBVU1NGBHBrZwNhOTdhYjJhNS01Mjc4LTM5ODAtODQ5MS03NzE0OGVjMGU0YWYEcG9zAzQEc2VjA3RvcF9zdG9yeQR2ZXIDMjhjMjNhNzA](http://news.yahoo.com/more-50-occupy-protesters-arrested-york-005726648.html;_ylt=AoKhxZ16PZLhp2CNMZgCIJlvzwcF;_ylu=X3oDMTNucXRyaDBvBG1pdANUb3BTdG9yeSBVU1NGBHBrZwNhOTdhYjJhNS01Mjc4LTM5ODAtODQ5MS03NzE0OGVjMGU0YWYEcG9zAzQEc2VjA3RvcF9zdG9yeQR2ZXIDMjhjMjNhNzA)

**(New Jersey) Bomb squad called to disable device found at Ringwood shopping center.** An officer's investigation into a faulty brake light ended in the evacuation of a Ringwood, New Jersey shopping center and the arrest of a man accused of making a bomb found in the car December 14, authorities said. The officer followed the car as it drove into the Fieldstone shopping center where it parked, and the officer kept driving a short distance until his computer showed the license plate was stolen off another vehicle. The officer went back to the parked car and found what appeared to be a 4-inch pipe bomb made from a white PVC pipe with a fuse. Police called the sheriff's office bomb squad during the hours-long investigation. Police shut down the shopping center for 3 hours. The bomb squad disabled the device, rendering it safe. Investigators did not find any additional explosives in the car and did not immediately find the car's owner. Detectives went to the home where the owner rents a room and found PVC piping, black powder, and fuse-making material similar to the fuse on the bomb in the car, the chief said. The suspect, whom investigators said was hiding in the woods behind the shopping center, contacted police, and turned himself in. Source:

[http://www.northjersey.com/news/crime\\_courts/Bomb\\_squad\\_called\\_to\\_disable\\_device\\_found\\_at\\_Ringwood\\_shopping\\_center.html](http://www.northjersey.com/news/crime_courts/Bomb_squad_called_to_disable_device_found_at_Ringwood_shopping_center.html)

## UNCLASSIFIED



## **COMMUNICATIONS SECTOR**

**(Oregon) Hundreds lose 911 service after thieves make off with copper phone lines.** Century Link said hundreds in Oregon were left without phone service December 18. Some were unable to call 911 after thieves made off with hundreds of feet of copper phone lines. The wire theft left parts of Douglas, Curry, and Coos County without phone service. They were alerted to the problem at 8 p.m. December 18 after their fiber optic cable began bouncing information back. They say they traced the problem to a portion of the line just outside of Tenmile. Officials said someone climbed a telephone pole and cut the cable, making off with an estimated 600 feet of copper cable. In the process they damaged a fiber optic line, the only outside connection Tenmile and Camas Valley have to the outside world, including 911. Officials said the outage was so severe, even a quick fix wasn't easy. They said they spliced the line temporarily on the ground so they could get those circuits up and operating. Century Link said all phone lines have been restored. Douglas County sheriff's deputies said within the last year, three separate phone line jackings have led to widespread outages. Source:

<http://www.kmtr.com/news/local/story/Hundreds-lose-911-service-after-thieves-make-off/icyVaeCc80uHltoraDJV4w.csp>

**It's official: LightSquared interferes with GPS.** The U.S. defense and transportation departments, along with the multiagency positioning, navigation and timing executive committee confirmed December 15 in identical statements that transmitters that start-up cellular company LightSquared plans to use for a national wireless broadband network caused "harmful interference to the majority" of general purpose Global Positioning System receivers in recent tests. LightSquared's plans also hit another speed-bump when the House approved an amendment to the 2012 National Defense Authorization Act barring the Federal Communications Commission from giving LightSquared the green light for commercial operation until Defense Department concerns about GPS interference from the company's network are resolved. In addition, the statement said, "separate analysis by the Federal Aviation Administration also found interference with a flight safety system designed to warn pilots of approaching terrain," but did not specify the system. A federal source who declined to be identified said FAA determined the LightSquared network caused interference with the GPS-enabled Enhanced Ground Proximity Warning System, which alerts pilots if they are too close to the ground. Preliminary analysis of test data showed the LightSquared transmitters caused "no significant interference with cellular phones" equipped with GPS chips, the statement said.

Source: [http://www.nextgov.com/nextgov/ng\\_20111215\\_8381.php](http://www.nextgov.com/nextgov/ng_20111215_8381.php)

## **CRITICAL MANUFACTURING**

**Recall: Hamilton Beach toasters—fire hazard.** Hamilton Beach Brands recalled about 14,000 classic chrome two-slice toasters because of a fire hazard, the Consumer Product Safety Commission announced December 15. When the toasters are first plugged into an outlet, the heating element can be energized although the toaster lifter is in the up or off position, which can pose a fire hazard if the toaster is near flammable items. Hamilton Beach received five reports of toasters being energized when first plugged into an outlet. There have been no

## UNCLASSIFIED

reports of injuries or property damage. The recalled toasters were sold at mass merchandisers and department, grocery, and home center stores nationwide from August through November. Some of the toasters were sent to consumers as replacements for model 22600 toasters recalled in June. Source: [http://news.consumerreports.org/recalls\\_safety/2011/12/recall-hamilton-beach-toastersfire-hazard.html?EXTKEY=I72RSSB](http://news.consumerreports.org/recalls_safety/2011/12/recall-hamilton-beach-toastersfire-hazard.html?EXTKEY=I72RSSB)

**NHTSA recall notice - Nissan Sentra battery terminal.** Nissan announced December 14 the recall of 33,803 model year 2010-2011 Sentra vehicles equipped with MR20 engines, manufactured from May 11, 2010 to May 22, 2010, and July 8, 2010 to October 25, 2010. The zinc coating applied to the terminal stud bolt was thicker than specification. This can result in a voltage drop that may cause difficulty starting the vehicle and could cause damage to the engine control module. This issue can cause the engine to stall while the vehicle is in motion and it may not be possible to restart the engine after it stopped, increasing the risk of a crash. Nissan will notify owners, and dealers will replace the positive battery terminal and cover. Source: [http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl\\_ID=11V579000&summary=true&prod\\_id=724828&PrintVersion=YES](http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=11V579000&summary=true&prod_id=724828&PrintVersion=YES)

## **DEFENSE/ INDUSTRY BASE SECTOR**

**San Antonio man caught selling military equipment to Arabs pleads guilty.** A San Antonio man, who told an undercover agent he was selling military equipment for the United Arab Emirates, pleaded guilty December 15 for illegally exporting military components. A U.S. attorney announced the week of December 12 that the man admitted before a federal judge he sold a Naval Radar Control Unit parts, and intended to sell more. The man, who regularly purchases and resells Department of Defense equipment, pleaded guilty to one count of illegally exporting military equipment. He admitted that beginning in May 2010, he sold a "sensitivity time control generator assembly," for an agreed-upon price of about \$6,500, and tried to sell more to an undercover U.S. Immigration and Customs Enforcement Homeland Security Investigations (ICE-HSI) agent. "These particular units are covered by the U.S. Munitions List and require a State Department license to export," states a DHS release. "According to court documents, the undercover agent told [the man] he was a broker for a buyer in the United Arab Emirates, and inquired as to how he would get the export license," it stated. "[The man] admitted that he knew he needed the license." He did not attempt to get a license, and used false information on shipping labels to disguise the actual contents. The man was arrested by ICE-HSI agents October 21 when he attempted to sell the other three units. He could receive up to 20 years in federal prison at his sentencing hearing, scheduled for February 24. He is on bond pending sentencing. Source: <http://www.examiner.com/headlines-in-san-antonio/san-antonio-man-caught-selling-military-equipment-to-arabs-pleads-guilty>

## **EMERGENCY SERVICES**

**(Connecticut) Justice Department says a Conn. police department targeted Latinos.** In a scathing report, the U.S. Department of Justice (DOJ) December 20 accused the East Haven

UNCLASSIFIED

## UNCLASSIFIED

Police Department (EHPD) in Connecticut of engaging in a pattern of widespread discrimination against Latinos in violation of the Constitution and federal law. The DOJ described the discrimination as “deeply rooted in the Department’s culture,” and cited a statistical analysis showing how Latinos were “intentionally targeted” for traffic stops. It provided the example of a particular officer’s stops — 40.5 percent of which were of Latino drivers. Overall, the investigation found that 19.9 percent of traffic stops made by the EHPD were of Latino drivers, concluding it “shows pervasive discrimination against Latinos on every level of EHPD traffic enforcement activity.” The report also said officers targeted Latinos by focusing on customers leaving Latino businesses. In addition to the high rate of traffic stops, the report accused some EHPD officers of conducting unauthorized immigration investigations. The DOJ said it will meet with community leaders, as well as with municipal agencies to address the concerns in the report. Source: [http://www.cnn.com/2011/12/19/us/connecticut-police-discrimination/index.html?hpt=us\\_c2](http://www.cnn.com/2011/12/19/us/connecticut-police-discrimination/index.html?hpt=us_c2)

**(Washington) Justice Department finds Seattle Police Department engaged in excessive force.** The Seattle Washington Police Department has used weapons either excessively or unnecessarily more than half the time during arrests, the U.S. Justice Department (DOJ) announced December 16. The finding was the result of a lengthy investigation that concluded the Seattle department engaged in a pattern of excessive force in violation of the Constitution and federal law. The investigation, which began in March, was conducted by the U.S. attorney’s office in Washington state along with the DOJ’s Civil Rights Division. DOJ investigators looked at a random sample of force reports between 2009 and 2011 and concluded when Seattle Police Department officers use force, they did so in an unconstitutional manner nearly 20 percent of the time. It found officers too quickly resorted to using impact weapons such as batons and flashlights. In an effort to restore public confidence and trust, the Seattle Police Department has begun to implement many remedial measures, including new force policies and training for officers on how to conduct effective and constitutional policing, according to the DOJ. Source: <http://www.cnn.com/2011/12/16/justice/washington-seattle-police/index.html>

**(Pennsylvania) 2 officers shot, 1 fatally, in Pa. traffic stop.** Authorities are searching for the man they say fatally shot a southwestern Pennsylvania police officer and wounded another in a shoot-out following a late-night traffic stop. State police in Washington County said the officer was fatally shot December 18 during a traffic stop on Interstate 70 in East Washington. A second officer was also wounded. The trooper said police were searching for a 58-year-old male in connection with the shooting. Police surrounded his home in Webster, Westmoreland County, early December 19 trying to serve a homicide warrant. They are asking anyone who knows his whereabouts to contact police. It was not immediately clear what prompted the traffic stop. Source: [http://www.ldnews.com/ci\\_19577121?source=most\\_viewed](http://www.ldnews.com/ci_19577121?source=most_viewed)

**(Arizona) Feds issue scathing report against Ariz. sheriff.** A scathing U.S. Justice Department (DOJ) report released December 15 found that the Maricopa County, Arizona’s sheriff’s office carried out a blatant pattern of discrimination against Latinos and held a “systematic disregard” for the Constitution amid a series of immigration crackdowns that turned the lawman into a prominent national political figure. The sheriff struck a defiant tone in response to the report,

UNCLASSIFIED

## UNCLASSIFIED

calling it a politically motivated attack by the U.S. President's administration that will make Arizona unsafe by keeping illegal immigrants on the street. The government found the sheriff's office committed a wide range of civil rights violations against Latinos, including unjust immigration patrols and jail policies that deprive prisoners of basic Constitutional rights. The report will be used by the DOJ to seek major changes such as new policies against discrimination, and improvements of staff and officers. The sheriff faces a January 4 deadline for saying whether he wants to work out an agreement to make the changes. If not, the federal government will sue him, possibly putting in jeopardy millions of dollars in federal funding for Maricopa County. The fallout from the report was swift. The DHS announced it is severing its ties with the sheriff, stripping his jail officers of their federal power to check whether inmates in county jails are in the county illegally, a move that was meant to speed up deportation. Apart from the civil rights probe, a federal grand jury also has been investigating the sheriff's office on criminal abuse-of-power allegations since at least December 2009, and is specifically examining the investigative work of the sheriff's anti-public corruption squad. The DOJ said it had not yet established a pattern of alleged wrongdoing by the sheriff's office in the three areas where they will continue to investigate: complaints of excessive force against Latinos, botched sex-crimes cases, and immigration efforts that have hurt the agency's trust with the Hispanic community. Source: <http://news.yahoo.com/feds-issue-scathing-report-against-ariz-sheriff-050533368.html>

### **ENERGY**

Nothing Significant to Report

### **FOOD AND AGRICULTURE**

**E. Coli concern prompts Tyson ground beef recall.** Tyson Fresh Meats is recalling about 40,948 pounds of ground beef in 16 states because the meat may be contaminated with E. coli 0157:H7. In a recall alert issued December 16, the Dakota City, Nebraska-based company said the problem was discovered through routine Food Safety and Inspection Service testing, which confirmed a positive result for E. coli. The recall is of 10-pound chubs of "CHUCK FINE GROUND BEEF 80/20," packed in cases containing eight chubs (chubs are cylinders of ground beef). The beef was shipped to institutions and distributors in Alabama, California, Florida, Georgia, Illinois, Indiana, Kentucky, Louisiana, Mississippi, New York, North Carolina, Ohio, South Carolina, Tennessee, West Virginia, and Wisconsin. Source: <http://www.foodsafetynews.com/2011/12/tyson-recalls/>

**Allergen alert: Milk ingredient in instant topping.** Ohio Processors of London, Ohio is recalling its Instantwhip B/C Topping from food service distributors because the product contains a milk ingredient (sodium caseinate) that was not disclosed on the label, Food Safety News reported December 19. The recall was initiated after it was discovered that a supplier had provided the wrong packaging. The recalled Instantwhip B/C Topping was sold to food service distributors in Ohio, Maryland, New York, Indiana, Pennsylvania, and Michigan. Source: <http://www.foodsafetynews.com/2011/12/allergen-alert-milk-ingredient-in-whip-topping/>

## UNCLASSIFIED

## UNCLASSIFIED

**USDA lacks proper IT security posture.** An inspector general (IG) found U.S. Department of Agriculture (USDA) systems and networks continue to have numerous flaws despite efforts to bolster the IT security posture, Federal Computer Week reported December 15. In the Federal Information Security Management Act audits for 2009 and 2010, the IG made 33 recommendations for bolstering overall security. By the end of 2011, the department had met only six of those recommendations, a new IG report noted. In 2009, the IG recommended the USDA focus its efforts on a select number of priorities, instead of trying to achieve numerous goals during a short period. The USDA and its agencies received recommendations on working together to identify and complete one or two critical objectives before moving onto the next priorities. Although the IG noted the USDA took a collaborative approach to address these problems, its efforts were not enough. For example, during 2010 and 2011, the USDA funded 14 separate projects with none fully implemented during 2011. Instead, funding was slashed and the majority of the projects were scaled back, pushing adoption dates further ahead, the report states. The IG found also that the USDA lacked policy and procedures to oversee systems that contractors operated on agencies' behalf. Source: <http://fcw.com/articles/2011/12/15/flawed-it-security-program-at-usda.aspx>

**(Northeast) 14 ill in Salmonella outbreak linked to ground beef.** Fourteen people were confirmed infected with an antibiotic-resistant strain of Salmonella in an outbreak that led to a recall of ground beef from a Northeastern chain of grocery stores. In a news alert issued December 16, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) said Hannaford, a Scarborough, Maine-based grocery chain, is recalling an undetermined amount of fresh ground beef that may be contaminated with Salmonella Typhimurium. The various packages of ground beef were prepared and sold at Hannaford stores throughout Maine, Massachusetts, New Hampshire, New York, and Vermont. The link between the illness outbreak and the Hannaford ground beef is based on "epidemiologic and traceback investigations, as well as in-store reviews," according to the FSIS, which is working with the Centers for Disease Control (CDC) and its state health partners. Because of what it called "Hannaford's limited records," the FSIS said it has not determined who supplied the beef to the grocery chain. The FSIS said the CDC reported 14 infected people. Eleven of those individuals reported consuming ground beef. Ten of the 14 case-patients said they had purchased ground beef at Hannaford stores between October 12 and November 20. Source: <http://www.foodsafetynews.com/2011/12/14-ill-in-salmonella-outbreak-linked-to-ground-beef/>

**(Texas) Texas drought takes cow numbers down by 600K.** The worst drought in Texas' history has led to the largest-ever 1-year decline in the leading cattle-state's cow herd, raising the likelihood of increased beef prices as the number of animals decline and demand remains strong, the Associated Press reported December 16. Since January 1, the number of cows in Texas dropped by about 600,000, a 12 percent decline from the roughly 5 million cows the state had at the beginning of 2011, said a man who monitors beef markets for the Texas AgriLife Extension Service. The man said many cows were moved, but others were slaughtered. He said in Texas, Oklahoma, New Mexico, Louisiana, and Arkansas, about 200,000 more cattle

## UNCLASSIFIED

were slaughtered in 2011, a 20 percent increase over 2010. Source:

<http://news.yahoo.com/texas-drought-takes-cow-numbers-down-600k-082208305.html>

## **GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)**

Nothing Significant to Report

## **INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

**KOOBFACE botnet uses TDS to ensure a bigger profit.** The KOOBFACE botnet, known for using pay-per install and pay-per click mechanisms to help its controllers earn millions, was recently upgraded with a sophisticated traffic direction system (TDS) that handles all traffic referenced to affiliate Web sites. According to Trend Micro researchers, the TDS redirects traffic to locations that earn crooks affiliate cash for each user they fool into accessing the sites. Since Google implemented some security mechanisms that make sure botnets can no longer create fake e-mail accounts useful for spamming and creating social media profiles, the cybercriminals began relying on Yahoo! Mail. Once the e-mail accounts are made, the botnet uses them to create other accounts on social networking sites such as Twitter, Tumblr, FriendFeed, FC2, livedoor, So-net, and Blogger. In the third part of the process, images are collected with the help of a new binary component that gathers pictures of celebrities, cars, and anything else that might attract unsuspecting users. In the next stage, dedicated pieces of malware begin creating blog accounts and retrieve content for them from the command and control server. The posts from these rogue blogs are designed specifically to make sure they will pop up among the first results in search engines. By using an obfuscated JavaScript code that references the botnet's TDS domain, they are able to track the number of visits to each rogue blog post and redirect victims to the affiliated sites that help them earn money. To make sure as many Internet users as possible land on their Web sites, social media sites are also flooded with links. Source: <http://news.softpedia.com/news/KOOBFACE-Botnet-Uses-TDS-to-Ensure-a-Bigger-Profit-241896.shtml>

**Atari and Square Enix cough to exposing users' privates.** Atari apologized to gamers following a security breach that exposed their names and e-mail addresses, leaving users at heightened risk of spam. The gaming company blamed the minor breach (no credit cards or mobile phone numbers were exposed) on problems introduced during a migration to a new cloud-based server platform. Separately, game developer Square Enix admitted the weekend of December 17 and 18 that it lost up to 1.8 million user data records to attackers including names, addresses, and phone numbers following a hack attack on its Web site. Personal details of gamers in the United States and Japan spilled as a result of the breach at Square Enix, which also did not involve credit card details. Source: [http://www.theregister.co.uk/2011/12/20/atari\\_gaming\\_security\\_fail/](http://www.theregister.co.uk/2011/12/20/atari_gaming_security_fail/)



## UNCLASSIFIED

**Security mandates aim to shore up shattered SSL system.** A consortium of companies published a set of security practices they want all Web authentication authorities to follow for their secure sockets layer (SSL) certificates to be trusted by browsers and other software. The baseline requirements, published the week of December 12 by the Certification Authority/Browser Forum, are designed to prevent security breaches that compromise the tangled Web of trust that forms the underpinning of the SSL certificate system. Its release follows years of mismanagement by individual certificate authorities permitted to issue credentials trusted by Web browsers. Most notable is this year's breach of DigiNotar, which led to the issuance of a fraudulent certificate used to snoop on 300,000 Gmail users in Iran. Source: [http://www.theregister.co.uk/2011/12/17/ssl\\_certificate\\_security\\_requirements/](http://www.theregister.co.uk/2011/12/17/ssl_certificate_security_requirements/)

**Old smartphones leave tons of data for digital dumpster divers.** A recent exploration made by a digital forensics company into a handful of phones found in the smartphone secondary market showed how easy it is to glean information from old or lost phones, even if a factory reset has been committed. An expert from Access Data gave Dark Reading information on his findings from his informal research and explained some of the repercussions for corporations and consumers who do not pick, manage, or dispose of their phones wisely. The director of mobile forensics for AccessData said, "I'd guess if you went and grabbed 10 phones [from recycling companies], 60 percent are going to contain data." He said at the behest of a customer interested in the data lingering on phones sold by used phone resellers and consumers using Craigslist and eBay, he used AccessData's tools to do an in-depth forensics dive into five handsets acquired from this market. The phones were the iPhone 3G, Sanyo 2300, HTC Wildfire, LG Optimus, and HTC Hero. Of those five, the iPhone and the old Sanyo had not been reset and contained what the director called logical data — active account sign-ons, contacts, and calendar information easily usable by any person who turns on the phone. Even though all of the Android phones had been wiped through a factory reset, four of the five phones also included data that would take someone with forensics tools and knowledge to extract from more hidden storage locations. Some of the details available within those phones included user account information, Social Security numbers, geo-location tags, deleted text messages, and a resume. Source: <http://www.darkreading.com/security/news/232300628/old-smartphones-leave-tons-of-data-for-digital-dumpster-divers.html>

## **NATIONAL MONUMENTS AND ICONS**

Nothing Significant to Report

## **POSTAL AND SHIPPING**

Nothing Significant to Report

## UNCLASSIFIED

## **PUBLIC HEALTH**

**Drug Shortages: FDA's ability to respond should be strengthened.** The U.S. Government Accountability Office (GAO) released a study December 15 that found the number of drug shortages has grown substantially in recent years, and the Food and Drug Administration (FDA) is constrained in its ability to protect the public health from the impact of these shortages. In total, 1,190 shortages were reported from January 1, 2001 through June 20, 2011, according to University of Utah Drug Information Service data. From 2006 through 2010, the number of drug shortages increased each year and grew by more than 200 percent over this period. A record number of shortages (196) were reported in 2010, and 2011 is on pace to surpass 2010's record, with 146 shortages reported through June 20. Twelve of the 15 drug shortages GAO reviewed in detail were primarily caused by manufacturing problems, including those that resulted in manufacturing shutdowns, according to information provided by the FDA and by manufacturers. The GAO found the FDA is constrained in its ability to protect public health from drug shortages. Specifically, FDA is constrained by its lack of authority to require manufacturers to provide the agency and the public with information about shortages, or require that manufacturers take certain actions to prevent, alleviate, or resolve shortages. Source: <http://www.gao.gov/products/GAO-12-315T>

**Heart device parts recalled.** St. Jude Medical said December 15 its Riata defibrillator leads, which the company stopped selling last year, had been recalled by the Food and Drug Administration (FDA) because of their potential to injure or kill patients. The devices remain implanted in an estimated 79,000 patients, St. Jude said. The company voluntarily sent a letter to doctors November 28 informing them the wires, which are used to connect the devices to the heart, had a higher failure rate than was previously known. The FDA deemed the letter a Class 1 recall, its most serious designation, because of its potential risks. The wires inside some leads can penetrate the insulation, compromising the device's integrity. The devices may inappropriately shock some patients and fail to deliver necessary therapy to others. Source: [http://www.nytimes.com/2011/12/16/business/fda-recalls-faulty-leads-in-heart-device.html?\\_r=1](http://www.nytimes.com/2011/12/16/business/fda-recalls-faulty-leads-in-heart-device.html?_r=1)

## **TRANSPORTATION**

Nothing Significant to Report

## **WATER AND DAMS**

**(New Hampshire)** Crack in floor of Rochester water tower suspected in leak: Scare closed area for a quarter-mile around, forced evacuation of 1,000. Public works crews in Rochester, New Hampshire, determined the likely cause of a water tower leak December 13, which drew an emergency response from several communities and evacuated nearly 1,000 people for more than 8 hours, was a single crack on the steel floor at the base of the tank. According to a city engineer, while the cause of the leak is still being looked into, so far no other cracks or holes have been found. Crews placed large stones around the base of the tank December 13, where a

## UNCLASSIFIED

ring of water still sat, to try to bind soil together and prevent any movement. On December 14, crews were back at the tower using a small pump to remove the last few inches of water from the tank, and evaluations were done of the soil around the tank, which officials said was "liquified" by the floodwaters from the leak. No cracks were found in the pipe that leads into the tower, officials said, nor any on the interior of the tank shell. The fuel pipe and mixer equipment, some of which was added in during a refurbishment project 3 years ago to improve water quality, also did not appear to be damaged. The soil around the tank was still holding up as of December 15, the city engineer said, adding the tank had not moved at all since the leak. Source:

[http://www.fosters.com/apps/pbcs.dll/article?AID=/20111216/GJNEWS\\_01/712169936](http://www.fosters.com/apps/pbcs.dll/article?AID=/20111216/GJNEWS_01/712169936)

### **NORTH DAKOTA HOMELAND SECURITY CONTACTS**

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **North Dakota State and Local Intelligence Center:** 866-885-8295(IN ND ONLY); Email: [ndslic@nd.gov](mailto:ndslic@nd.gov); Fax: 701-328-8175 **State Radio:** 800-472-2121; **Bureau of Criminal Investigation (BCI):** 701-328-5500; **North Dakota Highway Patrol:** 701-328-2455; **US Attorney's Office Intel Analyst:** 701-297-7400; **Bismarck FBI:** 701-223-4875; **Fargo FBI:** 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security [kihagel@nd.gov](mailto:kihagel@nd.gov), 701-328-8168

UNCLASSIFIED